



## PATENT ABSTRACTS OF JAPAN

(11) Publication number: **09054547 A**(43) Date of publication of application: **25.02.97**

(51) Int. Cl.

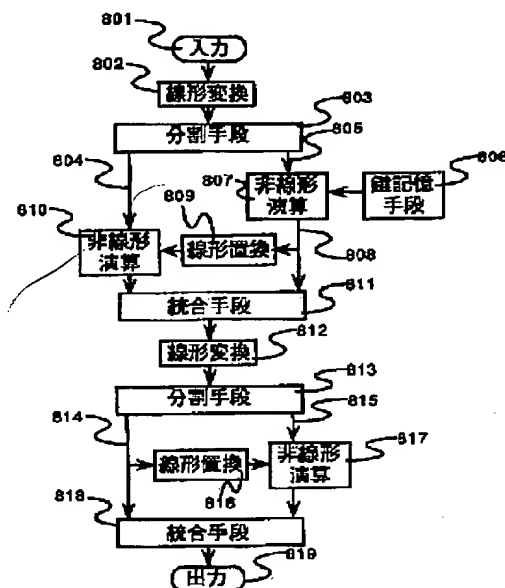
**G09C 1/00****H04L 9/06**(21) Application number: **07206372**(71) Applicant: **NEC CORP**(22) Date of filing: **14.08.95**(72) Inventor: **MIYANO HIROSHI**(54) **CIPHER DEVICE**

## (57) Abstract:

**PROBLEM TO BE SOLVED:** To provide a cipher device having high safety for safeguarding data at the time of communication and storage of the data.

**SOLUTION:** Input 801 is divided to a bit string 805 and bit string 804 by a dividing means 803 after linear conversion 802. The bit string 805 is the input together with a key storage means 806 to nonlinear arithmetic operation 807. Linear substitution 809 is inputted with the output 808 of the nonlinear arithmetic operation 807 and nonlinear arithmetic operation 810 is inputted with the output of the linear substitution 809 and the bit string 804. The output 808 and the output of the nonlinear arithmetic operation 810 are integrated by an integrating means 811 and the output receives linear conversion 812 and is divided to a bit string 815 and a bit string 814 by a dividing means 813. The bit string 814 is subjected to nonlinear arithmetic operation 817 together with the output 815 after linear substitution 816 with a direct integrating means 818 and is inputted to the integrating means 818, by which the bit string is integrated to output 819.

COPYRIGHT: (C)1997,JPO



(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平9-54547

(43)公開日 平成9年(1997)2月25日

(51)Int.Cl. <sup>6</sup>	識別記号	庁内整理番号	F I	技術表示箇所
G 0 9 C 1/00	6 1 0	7259-5 J	G 0 9 C 1/00	6 1 0 C
H 0 4 L 9/06			H 0 4 L 9/00	6 1 1 B

審査請求 有 請求項の数 3 O L (全 9 頁)

(21)出願番号 特願平7-206372

(22)出願日 平成7年(1995)8月14日

(71)出願人 000004237

日本電気株式会社

東京都港区芝五丁目7番1号

(72)発明者 宮野 浩

東京都港区芝五丁目7番1号 日本電気株式会社内

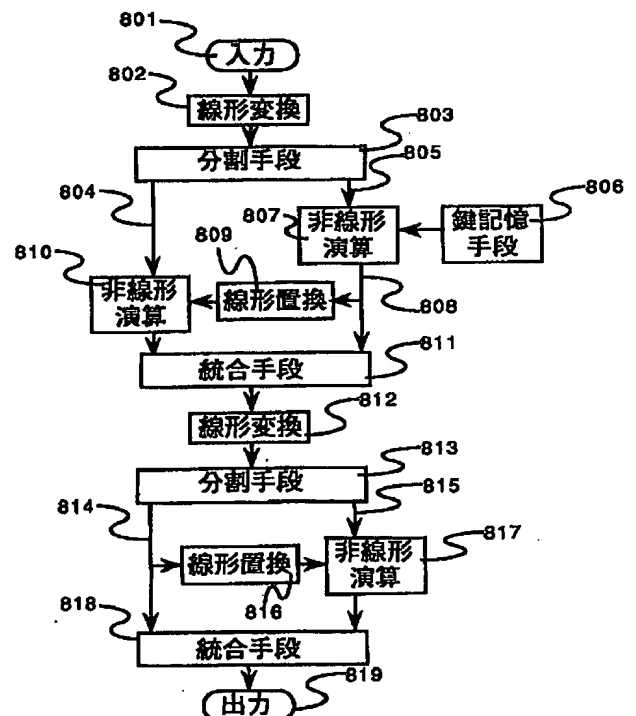
(74)代理人 弁理士 京本 直樹 (外2名)

#### (54)【発明の名称】 暗号装置

(57)【要約】 (修正有)

【課題】 データの通信や蓄積の際にデータを秘匿するための安全性の高い暗号装置を提供する。

【解決手段】 入力801は線形変換802後、分割手段803でビット列805とビット列804に分割される。ビット列805は、鍵記憶手段806とともに非線形演算807の入力となる。線形置換809は非線形演算807の出力808を入力し、非線形演算810は線形置換809の出力とビット列804を入力する。出力808と非線形演算810の出力は統合手段811で統合され、出力は線形変換812を受け、分割手段813でビット列815とビット列814に分割される。ビット列814は直接統合手段818と、線形置換816の後、出力815と共に非線形演算817されて統合手段818へ入力して統合され、出力819となる。



## 【特許請求の範囲】

【請求項1】入力データを鍵に依存して暗号化する暗号装置であって、入力データを複数の同一データ長の部分データに分割する第1の分割手段と、複数のデータ攪拌手段と、複数の同一データ長の部分データを統合する第1の統合手段を有し、前記各々のデータ攪拌手段は、前記部分データの少なくとも1つを入力とし、該部分データと同一のデータ長のデータを出力とし、内部に有する鍵記憶手段内に記憶された鍵に依存したデータ変換処理を行うデータ変換手段を少なくとも1つ有し、該データ変換手段の出力を複数の部分データの1つに作用させることを特徴とする暗号装置において、

前記データ変換手段が、鍵を記憶する鍵記憶手段と、前記データ攪拌手段の入力に線形変換を施す第1の線形変換手段と、該第1の線形変換手段の出力をそれぞれ同一の長さの第1のビット列と第2のビット列に分割する第2の分割手段と、該第1のビット列に前記鍵記憶手段に記憶された鍵を作用させて非線形演算を行う第1の非線形演算手段と、該第1の非線形演算の出力に線形置換を施す第1の線形置換手段と、前記第2のビット列に該第1の線形置換手段の出力を作用させて非線形演算を行う第2の非線形演算手段と、前記第1の非線形演算手段の出力と該第2の非線形演算手段の出力とを連結してひとつのビット列とする第2の統合手段と、該第1の統合手段の出力に線形変換を施す第2の線形変換手段と、該第2の線形変換手段の出力をそれぞれ同一の長さの第3のビット列と第4のビット列に分割する第3の分割手段と、該第4のビット列に線形置換を施す第2の線形置換手段と、前記第3のビット列に該第2の線形置換手段の出力を作用させて非線形演算を行う第3の非線形演算手段と、該第3の非線形演算手段の出力と前記第4のビット列とを連結してひとつのビット列として出力する第3の統合手段とを備えることを特徴とする暗号装置。

【請求項2】請求項1に記載の暗号装置において、前記データ変換手段が、第3の統合手段の出力と前記鍵記憶手段に記憶された鍵とを入力として該鍵と同一のビット長のデータを生成し該生成されたデータを前記鍵記憶手段に記憶させる鍵更新手段を備えることを特徴とする暗号装置。

【請求項3】請求項1又は請求項2に記載の暗号装置において、データ変換手段の有する線形変換手段の少なくとも1つが、該線形変換手段の入力を入力とする線形置換手段と、該線形置換手段の出力と前記線形変換手段の入力とを入力とする演算手段とを備えることを特徴とする暗号装置。

## 【発明の詳細な説明】

## 【0001】

【産業上の利用分野】本発明は、データの通信や蓄積の際にデータを秘匿するための暗号装置に関する。

## 【0002】

【従来の技術】DES (Data Encryption Standard) と呼ばれる暗号方式 (特開昭51-108701号公報「暗号装置」) に代表される共通鍵暗号の多くは、比較的簡単な変換操作を繰り返し行うことによって複雑な暗号化変換を実現することの特徴としている。図1は、多くの共通鍵暗号方式に採用されている暗号化手順の代表的な例を示したブロック図である。

10 【0003】入力されたテキスト101は、分割手段102において第1のテキスト103と第2のテキスト104に分割される。この例においては、入力101が直ちに分割手段102の入力となっているが、入力に線形置換を施したり、あるいは暗号鍵に基づいて生成されたビット列とのビット毎の排他的論理和をとるなど、入力101に何らかの可逆な処理をほどこしたものを分割手段102の入力とするような構成をとるような暗号方式もある。第1のテキスト104および第2のテキスト104は攪拌手段105の入力となる。攪拌手段105による処理を繰り返された後、統合手段106は攪拌手段によって攪拌された第1の攪拌済みテキスト109と第2の攪拌済みテキスト110とを統合して出力111とする。前記攪拌手段105はデータ変換手段107を内蔵し、該変換手段107の出力と前記第2のテキストとのビット毎の排他的論理和をとった値で第2のテキストが置き換えられる。

20 【0004】このような構成をとる暗号方式としては、DES以外には、FEAL (宮口庄司ら“Fast data encryption algorithm FEAL-8”, Review of electrical communications laboratories, Vol. 36 No. 4, 1988) などが提案されている。

【0005】これらの暗号方式は、データ変換手段107の内部構造によって特徴づけられる。

【0006】図2はDESのデータ変換手段107の構成を示したものである。図2を用いてDESのデータ変換手段の構成を説明する。

40 【0007】32ビットからなるデータ変換手段の入力201は、拡大転置E202によって48ビットに拡張される。この48ビットと、鍵記憶手段202に記憶されている48ビットの鍵との間でビット毎の排他的論理和204が計算される。非線形関数部205はS<sub>1</sub>からS<sub>8</sub>までの8つの非線形関数からなる。それぞれの非線形関数はいずれも入力ビット長が6ビット、出力ビット長が4ビットである。排他的論理和204の出力48ビットは、先頭から順に6ビット毎、8つの部分に区切られ、それぞれ順にS<sub>1</sub>, S<sub>2</sub>, ..., S<sub>8</sub>の入力となる。8つの非線形変換の出力の合計32ビットは、転置P206によって転置され、その結果が出力207とな

る。

【0008】図3は拡大転置E202の機能を表した表である。拡大転置E202は入力長32ビット、出力長48ビットの関数である。この表は、たとえばこの表の先頭の「32」という数字は拡大転置E202の出力の最初のビットは入力の32番目と一致することを表しており、この表の2番目の「1」という数字は拡大転置E202の出力の2番目のビットは入力の1番目と一致することを表しているというように、拡大転置E202の出力の48ビットと入力の32ビットの関係を表している。

【0009】図4は図3の非線形関数部205の8つの非線形関数 $S_1, S_2, \dots, S_8$ のうち、 $S_1$ の機能を表した表である。他の7つの非線形関数も、 $S_1$ と同様にあらかじめ定められた表によって機能が規定されているが、ここでは $S_1$ の機能を規定した表の説明をすることによって、非線形関数部の概要の説明とする。各々の非線形変換205は入力長6ビット、出力長4ビットの関数である。4つの行はそれぞれ、入力の先頭のビットと最後のビットの組がそれぞれ(0, 0)、(0, 1)、(1, 0)、(1, 1)である場合に対応している。16個の列はそれぞれ、入力の第2ビットから第5ビットまでの4つのビットを4桁の二進数とみなしたときに、この二進数が表している数字が0, 1, 2, ...である場合に対応している。表の各数字は、出力の4ビットを4桁の二進数とみなしたときの値を表している。たとえば、入力が(000000)であるとする、先頭のビットと最後のビットの組が(0, 0)であるからこれは表の一番上の行に対応し、第2ビットから第5ビットまでの4つのビットの組は(0000)でありこれを4桁の二進数と見ると0に対応するので該当する行の先頭の列が対応するから、その部分に書かれている数字「14」に対応する4桁の二進数(1110)が入力(000000)に対応する出力である。このように、入力に対応する出力が表によって定められているのがDESのデータ変換手段107の非線形関数 $S_1, S_2, \dots, S_8$ の特徴である。

$$S_0(x, y) = \text{rot}_2(x+1 \bmod 256)$$

$$S_1(x, y) = \text{rot}_2(x+y+1 \bmod 256)$$

ただし、上の式で $\text{rot}_2$ は2ビット分のビットのローテーションを表す。

【0015】また、これらの既存の暗号方式に対して改良を施すことによって安全性を高めようとする研究も行われている。たとえば小山謙二ら“*How to Strengthen DES-like Cryptosystems against Differential Cryptanalysis*”, IEICE Trans. Vol. E76-A No. 1 Jan 1993などがこうした研究の一例である。

【0016】図7を用いて、前記小山らによって提案さ ※50

\* 【0010】図5は転置P206の機能を表した図である。転置P206は入力長32ビット、出力長32ビットの関数である。表の見方は図3の拡大転置E202の機能を表した表と同様で、たとえばこの表の先頭の「16」という数字は転置P206の出力の最初のビットは入力の16番目と一致することを表しており、この表の2番目の「7」という数字は転置P206の出力の2番目のビットとは入力の7番目と一致することを表しているというように、転置P206の出力の32ビットと入力の32ビットの関係を表している。

【0011】図6はFEALのデータ変換手段107の構成を示したものである。図6を用いてFEALのデータ変換手段の構成を説明する。

【0012】32ビットからなるデータ変換手段の入力601は、8ビットずつの4つの部分に分割される。これらのうちの2番目の8ビットと3番目の8ビットは、これら自身と鍵記憶手段602に記憶されている16ビットの鍵とのビット毎の排他的論理和で置き換えられ、さらに1番目の8ビットは自身と新たに置き換えられた2番目の8ビットとのビット毎の排他的論理和で置き換えられ、4番目の8ビットは自身と新たに置き換えられた3番目の8ビットとのビット毎の排他的論理和で置き換えられる。さらに、2番目の8ビットは自身と3番目の8ビットを入力とする非線形関数 $S_1$ 603の出力で置き換えられ、3番目の8ビットは自身と2番目の8ビットとを入力とする非線形関数 $S_2$ 604の出力で置き換えられ、1番目の8ビットは自身と2番目の8ビットとを入力とする非線形関数 $S_3$ 605の出力で置き換えられ、4番目の8ビットは自身と3番目の8ビットとを入力とする非線形関数 $S_4$ 606の出力で置き換えられ、これらの4つの8ビットが統合されて32ビットの出力607となる。

【0013】図6の非線形関数 $S_0, S_1$ は、いずれも8ビットからなる2つの入力と1つの出力をそれぞれ8桁の二進数とみなすと、それぞれ以下の式で表すことのできる関数である。

\* 【0014】

※れた方式を説明する。

【0017】図7の攪拌手段701および攪拌手段702は、図1における攪拌手段105に対応する。この方式は、それぞれの攪拌手段701、702同士の間、データの内容に応じて右半分と左半部分を交換する機能を有する交換手段を挿入することの特徴としている。図7では、ふたつの攪拌手段しか描かれていないが、通常はそれぞれの攪拌手段の間が図7に示した構成をとる。

【0018】攪拌手段701は、データ変換手段703と、該データ変換手段の出力とデータの右半分とのビット毎の排他的論理和をとる手段704からなることは、

図1の構成と同様である。データ変換手段703は、たとえば図2や図6で説明したような構成をとることができる。交換制御手段705はデータの左半分706とデータの右半分707とを参照し、たとえば‘0’であるビットが偶数個のときには左右を交換し奇数個の時には交換しないというようなあらかじめ定められた規則によってデータの左右を交換するかどうかを決定する。この決定に応じて、交換手段708はデータの左右を交換し、あるいは交換しない。交換する場合にはデータの左半分706は右半分710となり、右半分707は左半分709となる。交換しない場合にはデータの左半分706はそのまま左半分709となり、右半分707はそのまま右半分710となる。こうして交換手段708によって交換され、あるいは交換されないデータは次の段の攪拌手段702の入力となる。

【0019】図7に示した方式の他にも、既存の暗号を改良することによって安全性を高める方式が提案されている。たとえば、鍵記憶装置（図2の202や図6の602）に記憶された鍵を、1ブロック（64ビット）暗号化する毎に更新することによって安全性を高める方式（特開平06-266284号公報（特願平05-050276号）「暗号化装置」）などである。

#### 【0020】

【発明が解決しようとする課題】前記DESなどの従来の暗号技術に対していくつかの解読法（暗号を破る手法）が提案されている。代表的なものに差分解読法（Eli Bihamら“Differential Cryptanalysis of DES-like Cryptosystems”, proceedings of CRYPTO'90）や線形解読法（松井充「DES暗号の線形解読法（I）」、1993年暗号と情報セキュリティシンポジウムSCIS93-3C）などがある。

【0021】DESは、図2に示したデータ変換手段の各々の出力ビットがいずれも入力の6ビットと鍵の6ビットからしか影響を受けていないことが線形解読法による攻撃が効果的であるひとつの理由であることが報告されている（宮野浩「線形解読法に対して有利なF関数の構成法」、1995年暗号と情報セキュリティシンポジウムSCIS95-A4.3, 1995.）。FEALの場合には、非線形関数603, 604, 605, 606に加法を用いているため、出力ビットは多くの入力ビットから影響を受けるが、一部のビットから受ける影響は加算の際に連続して繰り上がりが起こった時のみに受ける影響であるためきわめて小さい影響となっている。そのため、FEALについても線形解読法に対してあまり安全性が高くなっていない。

【0022】このように、線形解読法に対する安全性が低い暗号方式に対して、図7を用いて説明したような方法などで安全性を高めた場合でも、データ変換手

段107を改良することによってさらに安全性を高くすることは可能である。

【0023】以上、説明したような理由によって、図1のような構成を持つ暗号方式において高い安全性を実現するようなデータ変換手段107を構成することが要請されている。

#### 【0024】

【課題を解決するための手段】本発明の暗号装置は、入力データを鍵に依存して暗号化する暗号装置であって、  
10 入力データを複数の同一データ長の部分データに分割する第1の分割手段と、複数のデータ攪拌手段と、複数の同一データ長の部分データを統合する第1の統合手段を有し、前記各々のデータ攪拌手段は、前記部分データの少なくとも1つとを入力とし、該部分データと同一のデータ長のデータを出力とし、内部に有する鍵記憶手段内に記憶された鍵に依存したデータ変換処理を行うデータ変換手段を少なくとも1つ有し、該データ変換手段の出力を複数の部分データの1つに作用させることを特徴とする暗号装置において、前記データ変換手段が、鍵を記憶する鍵記憶手段と、前記データ攪拌手段の入力に線形変換を施す第1の線形変換手段と、該第1の線形変換手段の出力をそれぞれ同一の長さの第1のビット列と第2のビット列に分割する第2の分割手段と、該第1のビット列に前記鍵記憶手段に記憶された鍵を作用させて非線形演算を行う第1の非線形演算手段と、該第1の非線形演算の出力に線形置換を施す第1の線形置換手段と、前記第2のビット列に該第1の線形置換手段の出力を作用させて非線形演算を行う第2の非線形演算手段と、前記第1の非線形演算手段の出力と該第2の非線形演算手段の出力とを連結してひとつのビット列とする第2の統合手段と、該第1の統合手段の出力に線形変換を施す第2の線形変換手段と、該第2の線形変換手段の出力をそれぞれ同一の長さの第3のビット列と第4のビット列に分割する第3の分割手段と、該第4のビット列に線形置換を施す第2の線形置換手段と、前記第3のビット列に該第2の線形置換手段の出力を作用させて非線形演算を行う第3の非線形演算手段と、該第3の非線形演算手段の出力と前記第4のビット列とを連結してひとつのビット列として出力する第3の統合手段とを備えることを特徴とする。

【0025】また本発明の暗号装置は、前記データ変換手段が、第3の統合手段の出力と前記鍵記憶手段に記憶された鍵とを入力として該鍵と同一のビット長のデータを生成し該生成されたデータを前記鍵記憶手段に記憶させる鍵更新手段を備えることを特徴とする。

【0026】また本発明の暗号装置は、データ変換手段の有する線形変換手段の少なくとも1つが、該線形変換手段の入力を入力とする線形置換手段と、該線形置換手段の出力と前記線形変換手段の入力とを入力とする演算手段とを備えることを特徴とする。

## 【0027】

【実施例】前記のように、図1のような構成を持つ暗号方式において高い安全性を実現するようなデータ変換手段107を構成することは重要な問題である。そのようなデータ変換手段を実現するためには、非線形関数の非線形効果がなるべく効率良くデータ全体に広がっていくように構成することが効果的である。本発明は、データ変換手段がこのような効果を持つように、データ変換手段内部に線形変換手段を組み込んでいる。以下、実施例に従って本発明を詳細に説明する。

【0028】図8は、本発明の第1の実施例におけるデータ変換手段107の構成を表した図である。まず、全体の構成について説明し、線形変換802、812、非線形演算807、810、817、線形置換809、816の機能については後で述べる。

【0029】該データ変換手段の入力801は線形変換手段802による処理を受けた後、分割手段803において第1のビット列804と第2のビット列805とに分割される。第1のビット列805は、鍵記憶手段806とともに第1の非線形演算手段807の入力となる。第1の線形置換809は該非線形演算807の出力808を入力とし、第2の非線形演算810は該第1の線形置換809の出力と前記2のビット列804とを入力とする。前記第1の非線形演算807の出力808と前記第2の非線形演算810の出力とは統合手段811で統合され、該統合手段811の出力は線形変換手段812において線形変換を受け、該線形変換手段812の出力は分割手段813において第3のビット列814と第4のビット列215とに分割される。第2の線形置換816は該第4のビット列815を入力とし、第3の非線形演算817は該第2の線形置換816の出力と前記第3のビット列814とを入力とする。該第3の非線形演算817の出力と前記第4のビット列815とは統合手段818で統合され、818の出力が該データ変換手段107の出力819となる。

【0030】線形変換802は、入力データをXとしたときに、たとえば $\text{rot}_{12}(X)$ とX自身とのビット毎の排他的論理和を出力する装置として構成することができる。ここで $\text{rot}_{12}$ とは、既に説明したように、12ビット分のビットのローテーションを表す。

【0031】図10は図8の線形変換812の一構成例を示した図である。この例では、線形置換手段の一例として巡回置換手段を、演算手段としてビット毎の排他的論理和を用いている。巡回置換手段502にて入力501を入力し $\text{rot}_{12}$ の演算を行い、この演算結果と入力501のビット毎の排他的論理和503を出力としている。この構成例の特徴は、出力から入力が一意に定まらないため、解析されにくという点である。

【0032】線形変換812は、入力データをXとしたときに、たとえば $\text{rot}_{11}$ と $\text{rot}_{22}(X)$ とX自身と

のビット毎の排他的論理和を出力する装置として構成することができる。

【0033】図11は図8の線形変換802の一構成例を示した図である。この例では線形置換手段の一例として巡回置換手段を、演算手段としてビット毎の排他的論理和を用いている。ここで、巡回置換手段402、403にてそれぞれ $\text{rot}_{11}$ 、 $\text{rot}_{22}$ の演算を行い、これらの演算結果と入力401のビット毎の排他的論理和404を出力としている。この構成例の特徴は、出力がちょうど3つの入力ビットの影響を受けるため、この線形変換手段をデータ変換手段内に組み込んだ場合、データ変換手段の各出力ビットに影響を与える入力ビットの数が大きくなることである。

【0034】非線形演算807、810、817は、ふたつの入力をX、Yとして、たとえば $X \text{ xor } Y \text{ xor } \text{rot}_1(X \text{ and } Y)$ を出力する装置として構成することができる。ここで、 $\text{xor}$ とはビット毎の排他的論理和を表し、 $\text{and}$ とはビット毎の論理積を表す。

【0035】線形置換809は、たとえば入力を7ビットローテーションする装置として構成することができる。

【0036】該実施例において、データ変換手段の出力819の32番目とデータ変換手段の入力801と鍵記憶手段806に記憶されている鍵との関係を式に表したのが次の式である。この式において、 $Y_{32}$ はデータ変換手段の出力819の32番目のビット、 $X_i$ はデータ変換手段の入力801のi番目のビット、 $K_i$ は鍵記憶手段806に記憶されている鍵のi番目のビットをそれぞれ表し、+は排他的論理和、\*は論理積を表すものとする。

$$Y_{32} = K_2 + K_4 + K_{13} + K_{16} + X_{10} + X_{19} + X_{20} + X_{21} + X_{28} + X_{29} + X_{32} + K_{15} * (X_9 + X_{20} + X_{31}) + K_3 * (X_8 + X_{19} + X_{29}) + K_1 * (X_6 + X_{17} + X_{27}) + K_{12} * (X_6 + X_{17} + X_{29}) + (K_1 + X_6 + X_{17} + X_{27} + K_{15} * (X_{10} + X_{21} + X_{32})) * (X_8 + X_{18} + X_{29}) + (K_1 + K_{12} + X_8 + X_{18} + X_{27} + X_{28} + X_{29} + X_{15} * (X_{10} + X_{21} + X_{32})) + (X_{16} + X_{10} + X_{21} + X_{32} + X_{15} * (X_9 + X_{20} + X_{31})) * (X_7 + X_{17} + X_{26}) + K_{11} * (X_5 + X_{11} + X_{32})) * (K_3 + K_{15} + X_8 + X_9 + X_{19} + X_{20} + X_{29} + X_{31} + K_{14} * (X_8 + X_{19} + X_{30}) + K_2 * (X_7 + X_{18} + X_{28}))$$

論理積は非線形な演算であり、出力ビットが非線形な演算による影響を多く受けることによって暗号方式の安全性が高まる。前記の式から、本発明のデータ変換手段の出力819のビットが多くの非線形な演算による影響を受けていることがわかる。このことは、線形変換手段802、818が、これらの線形変換手段の入力とこの入力に対して線形置換（この実施例においてはビットのローテーション）を施した結果とで演算（この実施例にお

いてはビット毎の排他的論理和)を施す構成であるため、非線形演算 807, 810, 817 による非線形な演算の効果が効率よく拡散していることによる。

【0037】図9は本発明の第2の実施例におけるデータ変換手段107の構成を表した図である。本実施例においては、該データ変換手段107の出力を得るに至る手順は図8に示した例と全く同じである。図8との差異は、本実施例においては鍵更新手段920が統合手段918の出力と鍵記憶手段906に記憶されている鍵とを入力として該鍵と同一のビット長のビット列を出力し、該出力を鍵記憶手段906に記憶するというものである。鍵更新手段920は、たとえば非線形演算907と同じ構成にし、鍵記憶手段906に記憶されている鍵と統合手段918の出力の上位16ビットとを入力とするように構成することができる。

#### 【0038】

【発明の効果】以上詳細に説明したように、本発明によれば、データの通信や蓄積の際にデータを秘匿するための安全性の高い暗号装置を得ることができる。

#### 【図面の簡単な説明】

【図1】多くの共通鍵暗号方式において採用されている暗号化手順の構成図である。

【図2】DESのデータ変換手段の構成図である。

【図3】DESのデータ変換手段における拡大転置Eの機能を示した図である。

【図4】DESのデータ変換手段における非線形変換のうちのひとつの機能を示した図である。

【図5】DESのデータ変換手段における転置Pの機能を示した図である。

【図6】FEALのデータ変換手段の構成図である。

【図7】既存の暗号方式の安全性を高める従来方式の特徴的部分を示した図である。

【図8】本発明の第1の実施例におけるデータ変換手段の構成図である。

【図9】本発明の第2の実施例におけるデータ変換手段の構成図である。

【図10】本発明の線形変換812の構成図である。

【図11】本発明の線形変換802の構成図である。

#### 【符号の説明】

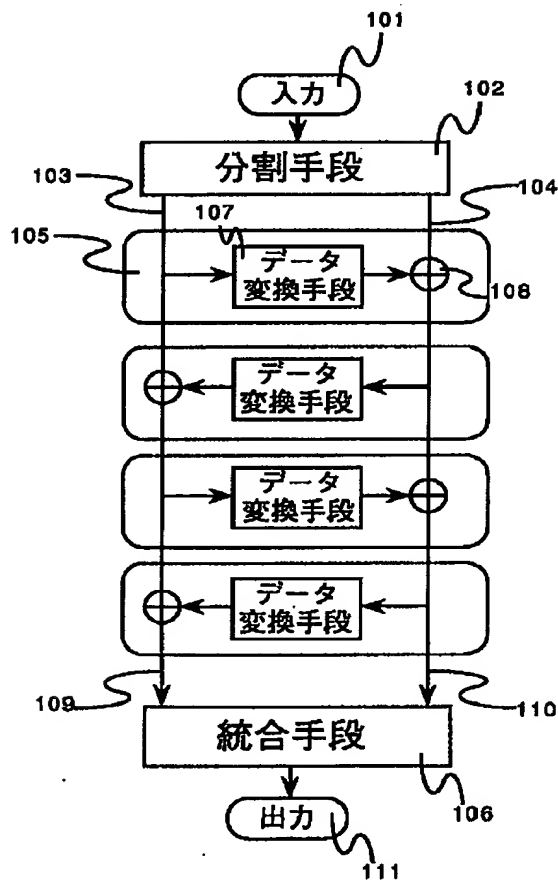
- 101 暗号装置の入力
- 102 第1のデータ分割手段
- 103 第1のテキスト
- 104 第2のテキスト
- 105 データ攪拌手段
- 106 第1のデータ統合手段
- 107 データ変換手段
- 108 ビット毎の排他的論理和
- 109 第1の攪拌済みテキスト
- 110 第2の攪拌済みテキスト
- 111 暗号装置の出力

- 201 データ変換手段の入力
- 202 拡大転置E
- 203 鍵記憶手段
- 204 ビット毎の排他的論理和
- 205 非線形関数部
- 206 転置P
- 207 データ変換手段の出力
- 401 入力
- 402 巡回置換手段1
- 10 403 巡回置換手段2
- 404 演算手段
- 405 出力
- 501 入力
- 502 巡回置換手段
- 503 演算手段
- 504 出力
- 601 データ変換手段の入力
- 602 鍵記憶手段
- 603 非線形関数S<sub>1</sub>
- 20 604 非線形関数S<sub>2</sub>
- 605 非線形関数S<sub>3</sub>
- 606 非線形関数S<sub>4</sub>
- 607 データ変換手段の出力
- 701 データ攪拌手段
- 702 データ攪拌手段
- 703 データ攪拌手段
- 704 ビット毎の排他的論理和
- 705 交換制御手段
- 706 データの左半分
- 30 707 データの右半分
- 708 交換手段
- 709 データの左半分
- 710 データの右半分
- 801 データの変換手段の入力
- 802 第1の線形変換
- 803 第2のデータ分割手段
- 804 第2のビット列
- 805 第1のビット列
- 806 鍵記憶手段
- 40 807 第1の非線形演算
- 808 第1の非線形演算207の出力
- 809 第1の線形置換
- 810 第2の非線形演算
- 811 第2のデータ統合手段
- 812 第2の線形変換
- 813 第3のデータ分割手段
- 814 第4のビット列
- 815 第3のビット列
- 816 第2の線形置換
- 50 817 第3の非線形演算

11

818 第3のデータ統合手段  
 819 データ変換手段の出力  
 901 データ変換手段の入力  
 902 線形変換  
 903 データ分割手段  
 904 ビット列  
 905 ビット列  
 906 鍵記憶手段  
 907 非線形演算  
 908 非線形演算307の出力  
 909 線形置換

【図1】



【図3】

拡大転置 E

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

【図4】

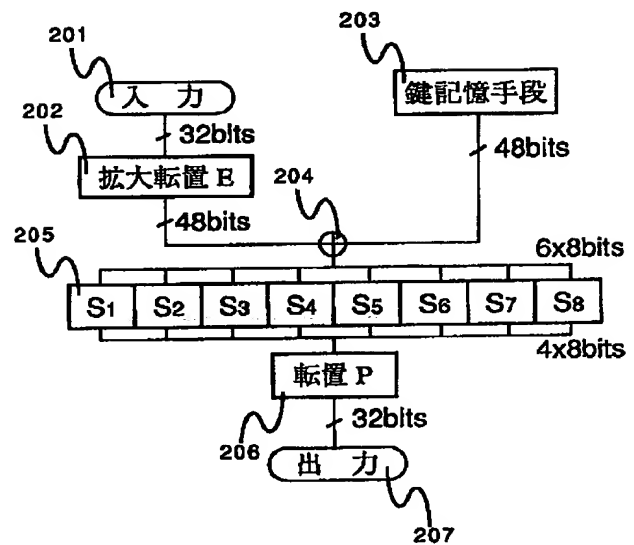
S<sub>1</sub> の関数表

14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

12

\* 910 非線形演算  
 911 データ統合手段  
 912 線形変換  
 913 データ分割手段  
 914 ビット列  
 915 ビット列  
 916 線形置換  
 917 非線形演算  
 918 データ統合手段  
 10 919 データ変換手段の出力  
 \* 920 鍵更新手段

【図2】



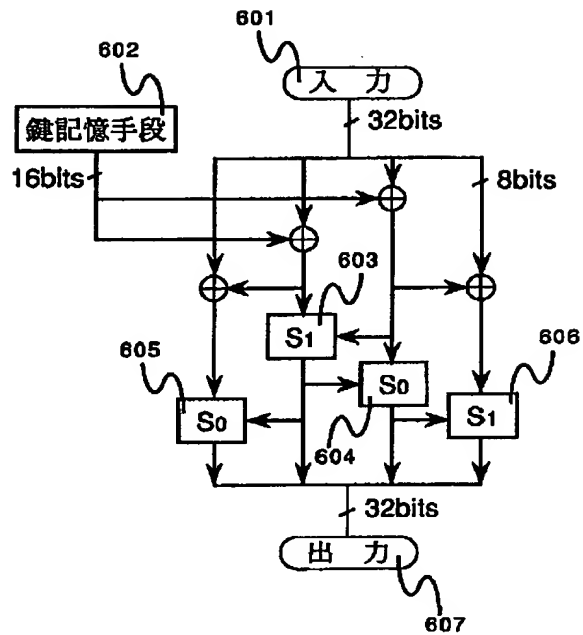
【図5】

転置 P

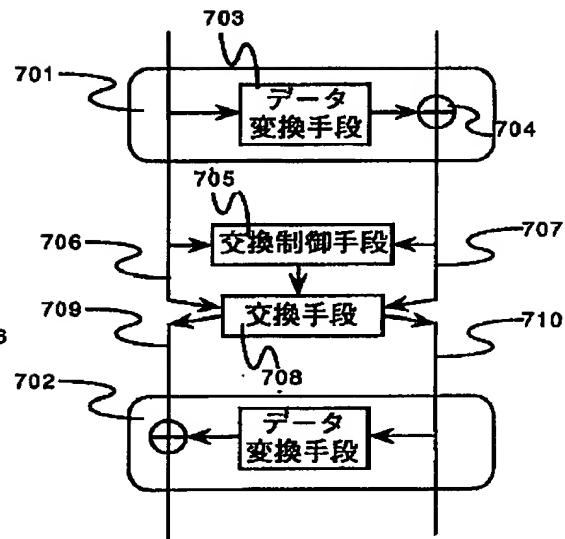
16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25



【図 6】

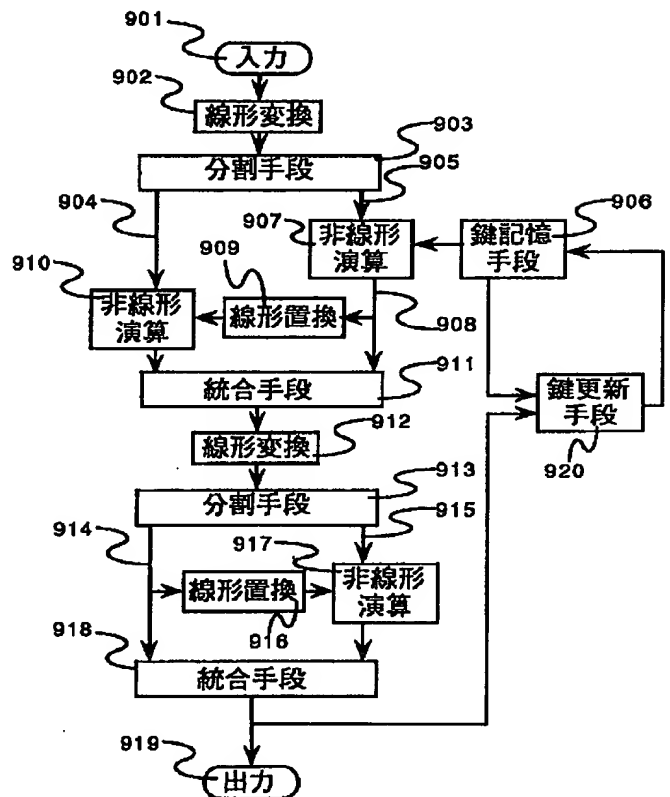
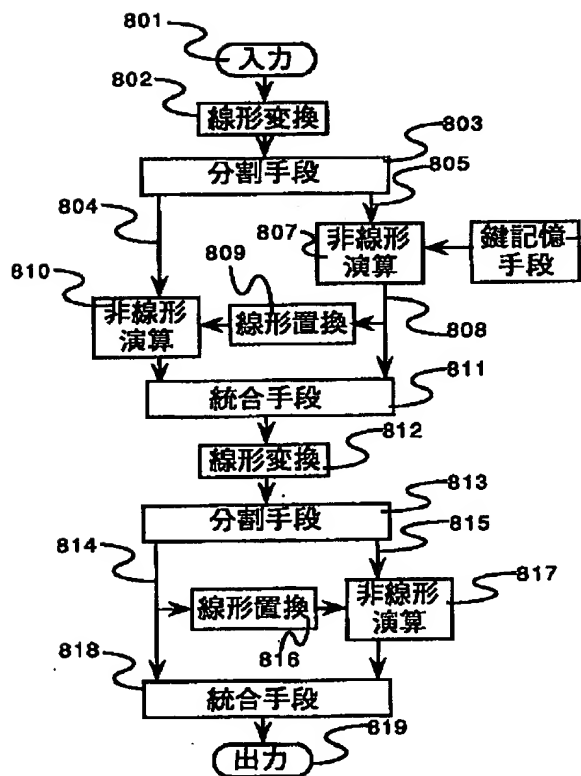


【図 7】

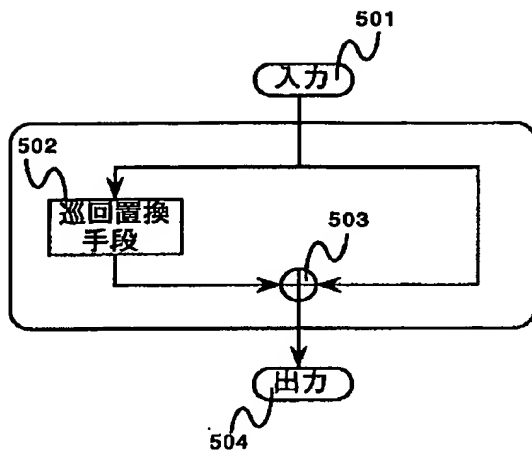


【図 9】

【図 8】



【図 10】



【図 11】

